PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04N 7/167

A2

(11) International Publication Number: WO 98/27731

(43) International Publication Date: 25 June 1998 (25.06.98)

(21) International Application Number: PCT/IB97/01534

(22) International Filing Date: 8 December 1997 (08.12.97)

(30) Priority Data:
08/768,492 18 December 1996 (18.12.96) US

(71) Applicant: PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(71) Applicant *(for SE only)*: PHILIPS NORDEN AB [SE/SE]; Kottbygatan 7, Kista, S-164 85 Stockholm (SE).

(72) Inventors: CAVALLERANO, Alan; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). BASILE, Carlo; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). GOLDENBERG, Jill, Forer; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: STEENBEEK, Leonardus, J.; Internationaal Octrooibureau B.V., P.O. Box 220, NL-5600 AE Eindhoven (NL).

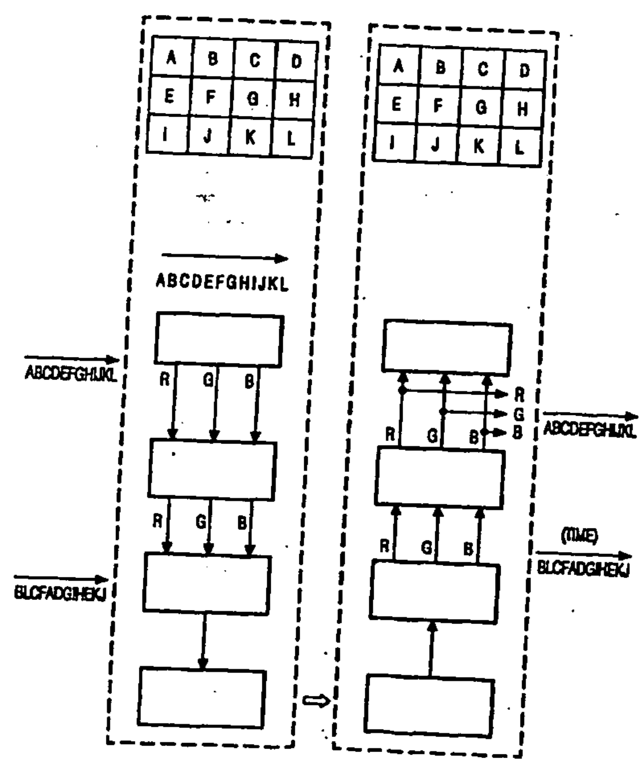
(81) Designated States: JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD AND DEVICE FOR PROVIDING CONTROLLED ACCESS VIDEO SIGNALS WITHOUT PROVIDING A SIGNAL IN THE CLEAR

(57) Abstract

An LCD display device for receiving encrypted video data and for decrypting the video data such that a signal is not provided "in the clear" before receipt by the display device. The video data is encrypted within a row of video and decrypted at the display. Alternatively the rows are encrypted by altering the time sequence of display of each row.



transmitter and is coupled to the MPEG Decoder (MPEG DEC). The RgB signals are still encrypted in a time sequence (T).

The MPEG Decoder is coupled with the Decryption-unit (DECR)

The Decryption-unit supplies the RgB signals is the original time sequence (DECR RSS T) to the Display (D) of the Receiver (R).

A video signal is often scrambled or encrypted so that without proper authorization, it is in an unusable form. However, if the consumer premises are granted authorization, then typically at interfaces which are accessible to the consumer, such as at the output of a cable converter box or the "video output" jacks of a receiver, the video signal is descrambled or decrypted and hence is "in the clear" (See Figure 3). In this figure Source Vides (SV) is supplied to the Encoder (ENC), which is coupled with the Encryption-unit (ENCR). The Encryption-unit supplies the encrypted signal to the Transmitter (TR). Via the Transmission Channel (TRCH0 is the signal supplied to the Receiver Input (RI), which Receiver Input is coupled to the Demodulator (DEM). The Demodulator is coupled to the Decoder (DEC). After decoding is the signal decrypted in the Decryption-unit (DECR) and supplied to the Output Port (OP). At this point the Video Signal (VS) is "in the clear" as mentioned earlier. The Output Port is coupled to the Monitor (M) with the display (D) and to the Video-Recorder (VCR). There are many types of display devices available today. There is the generally well known cathode ray tube display devices (CRT), and discrete display devices such as digital light modulators or deformable mirror spatial light modulator (DMD), liquid crystal displays (LCD), and plasma displays. Each of these displays have the problems associated with an unauthorized user simply recording the video "in the clear" from the output of the cable converter box or the "video output" jacks of a television receiver. For ease of description reference will be had to the operation of a LCD.

A liquid crystal display device includes liquid crystal picture elements ("pixels") arrayed in rows and columns. In an LCD display system, the discrete display device is illuminated on a "row" or line basis, due to the matrix addressing scheme typically employed. Hence, a particular row is illuminated and then another row is illuminated until an entire frame is created. For example, in a particular Philips LCD display device there are 480 columns by 480 rows worth of pixels. To load the 480 pixels required for a given row, column drivers are required. The 480 rows are then activated sequentially to create a picture (or a frame).

Fig. 4 shows a schematic diagram of an LCD display device. Referring to Fig. 4, the display device, which is intended to display video, for example television

pictures, includes an active matrix liquid crystal color display panel 10. The panel 10 comprises two spaced, transparent and insulating supporting plates, for example of glass, with twisted nematic liquid crystal disposed therebetween and has a large number of liquid crystal picture elements with associated switching elements and memory elements (e.g. capacitors) arranged in rows and columns which are addressed via first and second sets of crossing address conductors with each picture element being connected with a respective address conductor of each set. The first set comprises row address conductors extending in the row direction. Conductors of the second set extend generally in the column direction and hereinafter will be referred to as column address conductors. Each column address conductor is connected with a respective picture element in each row. In known active matrix liquid crystal display devices, the row address conductors serve as scanning electrodes and are controlled by a row driver circuit 15, comprising a shift register circuit, which applies a selection signal to each row conductor sequentially in turn during a respective row address period. In synchronism with the selection signals, achieved by means of the timing and control circuit 16, data (video) signals, obtained by sampling a TV line with serial to parallel conversion, are applied to the column address conductors from a column driver circuit 17 connected to the output of a video processing circuit 18 to produce a required display effect from the rows of picture elements as they are scanned. Thus the video information for a single line is loaded into the column driver circuit 17 and depending on the row addressed by the row driver circuit 15, this row is loaded with video information. The individual display effects of the picture elements, addressed one row at a time, combine to build up a complete picture in one field, the picture elements being addressed again in a subsequent field. This sequential loading of the array 10 provides a signal "in the clear" which is easily pirated.

It is an object of the invention to eliminate the signal "in the clear" in an LCD display device.

It is another object of the invention to eliminate the signal "in the clear" without requiring substantial modification of the LCD display device.

A further object of the invention is to eliminate the signal "in the clear" while minimizing temporal artifacts.

Achievement of these and other objects is based on the realization that to load the memory elements with pixel data it is not necessary to do so in a sequential order.

Instead the memory elements are loaded in an encrypted sequence in accordance with an encryption "key".

These objects are achieved in a first embodiment of the invention by encrypting the pixel data within a line or row of the display device and placing it in a register or other storage device of the column driver circuit and decrypting the pixel data by causing the register or other storage device to place decrypted data, decrypted in accordance with a decryption key, in the appropriate locations of the column driver circuit.

In a second embodiment of the invention, the row sequence or time order of the display of the rows is encrypted so that the row driver circuit must load the appropriate row in accordance with the decryption key.

In a third embodiment of the invention both the pixel sequence within a row and the row sequence are encrypted and both the row and column decoders load the LCD line by line in accordance with the encryption key.

In a fourth embodiment of the invention the encryption is performed to limit the temporal artifacts that occur due to varying the row sequence. This is achieved by partitioning each frame of video into a plurality of partitions. Each partition having the rows within the partition in an encrypted sequence but the time order of the display of the partitions is controlled.

Still other objects and advantages of the invention will in part be obvious and will in part be apparent from the specification.

The invention accordingly comprises the several steps and the relation of one or more of such steps with respect to each of the others, and the apparatus embodying features of construction, combinations of elements and arrangement of parts which are adapted to effect such steps, all as exemplified in the following detailed disclosure, and the scope of the invention will be indicated in the claims.

For a fuller understanding of the invention reference will be had to the following description taken in connection with the accompanying drawings, in which:

Figure 1 shows a typical MPEG display system.

Figure 2 shows a typical MPEG display system with encryption.

Figure 3 shows the availability of a signal in the clear in a MPEG encryption scheme.

Figure 4 is a diagram of a liquid crystal display device in accordance with

the invention.

Figures 5a-d show a preferred embodiment of the invention wherein the video sequence is partitioned into sections.

Figures 6a-c show the time allocation of the sections for each frame.

Figure 7a and b show a state diagram and table of the allowed transitions for the display shown in Figure 5c.

Figure 8 shows the flow of video data in a television receiver in accordance with the invention.

As explained above, the LCD embodiment shown in Figure 4 stores pixel data in the driver circuit 17. In the prior art, the column driver circuit 17 contains a number of memory elements corresponding to the number of active pixels on any given active line (row). The pixel data for a given line (row) are transferred to the array 10 in line-sequential order, under control of the line (row) driver circuit 15. The row driver circuit 15 addresses the row of picture elements in the array 10 for the desired line. The pixel data stored in the column driver circuit 17 are then transferred to array 10 line-by-line. The activation of the LCD occurs on a line-by-line basis which in succession creates a field (or frame) of video information. All of the timing for the system is under control of the timing and control circuit 16. The loading of the array can be referred to as a "write" operation, and the reading of the array corresponds to the a "read" operation, both are done on a line-by-line basis. The timing and control circuit 16 provides the appropriate write and read enable signals.

In an LCD system the pixel data must be loaded into the display array 10 on a line-by-line basis. Thus to avoid a "signal in the clear" in a first embodiment of the invention any encrypted video pixel data still must enter the LCD at least in a group that comprises a line, although within the line, the pixel data can be encrypted hence providing some level of security.

In a second embodiment of the invention the encrypting is also performed throughout the lines of the video, e.g. instead of the lines being activated sequentially 1-480, they are activated in a random order, e.g. 10, 400, 2, 276....., and a greater level of security is provided. There are some restrictions that must be imposed for this type of encryption in order to avoid temporal artifacts. Any given line that is activated for frame n, should not be activated for frame n+1 in a period of time that deviates too significantly from

the frame period. In other words, if line 251 is activated last in frame n, it should not be activated first in frame n+1 otherwise temporal artifacts can occur. The potential for temporal artifacts can be minimized by controlling the allowed line-by-line randomness of the encryption at the source by permitting encryption to take place within predetermined boundaries only. This limitation will guarantee the maximum and minimum intervals that any given line can be activated frame to frame. Figs. 5a-d depict such control of the encryption. Fig. 5a shows a typical display device. Figs. 5b and c show a preferred embodiment of the invention where the display device is broken up into predetermined boundaries denoted by sections A, B and C. Each section has a time order associated with it. In this example, section A is scanned first (1), section B is scanned second (2), followed by section C last (3). Assume section A contains pixel rows 1,2,3,4,5, section B contains pixel rows 6,7,8,9,10 and Section C contains pixel rows 11,12,13,14,15. This segregation of lines into sections takes place in theory at the encoder(transmission side), in anticipation of an LCD receiving the transmission. This is practical for implementations such as Electronic Cinema. In a first embodiment (Figs. 5c and d) of the invention the time order of the sections remains fixed, e.g. the rows of section A are activated first, rows of section B are activated second and rows of section C are activated third. The rows within each section are encrypted which provides a greater degree of protection from unauthorized users than merely encrypting the pixels within a row and there are little temporal artifacts which could arise. Thus section A can be encrypted by alternating the sequence of lines in Section A. For example, for frame 3, section A may transmit in time order rows 5,3,1,2,4 and in frame 8, the time order may be lines 2,3,4,1,5.

In another preferred embodiment of the invention a greater degree of randomness is permitted and thus a greater level of security. In this embodiment the sections A, B, and C are permitted to "swap" time allocations for a given frame but only by moving one section at a time. Reference is made to Figs 6a-c for this embodiment. Fig. 6a shows the time allocation of the sections for each frame. As can be seen from this figure, the time sequence for display of the partitions is not altered, section A is displayed first, section B is displayed second and section C is displayed third for each frame. Fig. 6b shows the time allocation of the sections for each frame when the sections are permitted to "swap" time allocations by moving one section at a time. Thus if section C appears third in frame 1 then it could appear third or second in frame 2 but not first. Similarly if section A appears first in frame 2 it can appear first or second in frame 3 but not third. Thus the temporal update rate for any given section is never allowed to deviate by more than a factor of one-third the

total frame period.

Fig. 7 shows a state diagram of the allowed transitions. In accordance with the invention the pixel data is not generated in time-sequential order because the data are encrypted and the time order of the pixels as they are output from the video decoder are in an encrypted sequence. Although the encrypted sequence appears random it still follows some type of "key". This means that the time order of the data might follow a pattern which would create a "scrambled" image where the pixels are not in the correct row sequential order or column sequential order and if the data were transferred to the array in a line-by-line pixel-by-pixel order the image would appear "scrambled." The pixel data would then be stored in the array of memory elements in apparently random locations. For example, assume the first pixel location is designated (0,0) for column 0 row 0, but, the pixel for the fourth column first row (4,1) is decoded for that location in the encrypted sequence. If the key is known, the data can be decrypted when it is loaded into the memory elements of the array 16 by column and row driver circuits 15 and 17 and then presented to the discrete display device for proper display.

Referring back to Fig. 4 and assuming sections A, B and C are displayed in the same time sequential order for each frame (Figs. 5a-d), the register within the column driver circuit 17 (not shown) will receive the first line of encrypted video for section A from the video processing circuit 18, e.g. row 1 if only the pixels within the row are encrypted and the time order of the rows within section A is sequential. The register will supply, in accordance with a decryption key, the column driver circuit 17 with the decrypted video data. The column driver circuit 17 will activate the columns of the array 10 and the row driver circuit 15 will activate row 1. If the encrypted sequence for row 1 is pixels 13, 12, 15, 14, 11 the column driver circuit's storage device or register (not shown) receives the encrypted video line and provides it decrypted to the column driver circuit 17. The column driver circuit then provides the pixel information directly to the display device in its appropriate sequence 11, 12, 13, 14, 15. Examples of such registers or storage devices include a register that serially loads the column driver circuit 17 in accordance with the encryption key, or a memory having address lines which are accessed by the column driver circuit 17 in accordance with the decryption key. If the rows are also in an encrypted time sequence the row driver circuit 15 will just activate the appropriate row in accordance with the decryption key before the column driver circuit 17 begins loading. Thus if the rows are to be activated in the order 5,3,1,2,4 rather than 1,2,3,4,5 the row driver circuit 15 must receive a decryption key so that instead of activating the rows sequentially it activates the

rows in the order 5,3,1,2,4.

Since the LCD displays pixels line-by-line it is not necessary that the lines be displayed sequentially as long as some restrictions are followed to limit temporal artifacts and as long as the pixels within the line are decrypted before display.

Figure 8 shows the flow of video data in a television receiver in accordance with the invention. The video is provided to a video encoder 30 for encoding and then to a encrypter 32. The encrypted and encoded video is then transmitted by transmitter 34 across the transmission channel to receiver 35. The receiver 35 supplies the encrypted and encoded video to video decoder 36. Although the video is decoded at video decoder 36, it is still in an encrypted form when it is supplied to the LCD display. The decryption occurs within the display device thus avoiding a signal in the clear at the video output jacks.

It will thus be seen that the objects set forth above, among those made apparent from the preceding description, are efficiently attained and, since certain changes may be made in carrying out the above method and in the construction set forth without departing from the spirit and scope of the invention, it is intended that all matter contained in the above description and shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.

CLAIMS:

1. A display device for decrypting and displaying encrypted video pixel data, comprising:

an array of p columns and l rows of pixel cells for displaying the decrypted video pixel data as a frame;

an array of p columns and l rows of corresponding memory elements each memory element being associated with a particular pixel cell and for storing digital code of the decrypted video pixel data which represents the luminance of the particular pixel cell during a frame period;

a register for storing at least a portion of a frame of the digital code of the encrypted video pixel data in an encrypted order rather than in a column and row sequential order;

a driver circuit for activating the rows and columns of the array of memory elements for loading the memory elements with the digital code stored in the register; and

a decrypter for i) receiving a decryption key, ii) supplying the decryption key to the register such that the driver circuit receives from the register a line of decrypted digital code and activates the columns of the array of memory elements, and iii) supplying the decryption key to the driver circuit such that the driver circuit activates the rows of the array of memory elements, one row at a time, non-sequentially in accordance with the decryption key.

2. The display device in accordance with claim 1, wherein the display device is a liquid crystal display device.

3. The display device in accordance with claim 1, further including a timing device for providing timing pulses to the driver circuit for activating the rows and columns of the array of memory elements.

4. The display device in accordance with claim 1, wherein the digital code itself is encrypted for each pixel cell and the decryption key decrypts the digital code from the register before supplying it to the driver circuit.

5. The display device: in accordance with claim 1, characterized in that the register is adapted for decrypting the line of digital code in accordance with a decryption

key;

and the driver circuit is adapted for receiving the decrypted digital code from the register.

6. The display device in accordance with claim 5, wherein the timing of the driver circuit for activating the rows and columns is provided by a timing circuit.

7. The display device in accordance with claim 1, characterized in that each frame of encrypted video data is received in predetermined partitions wherein the rows within each partition are displayed non-sequentially but the partitions are displayed sequentially.

8. The display device in accordance with claim 7, wherein the partitions are displayed non-sequentially.

9. The display device in accordance with claim 8, wherein the partitions are displayed non-sequentially in accordance with a time order from frame to frame that minimizes temporal artifacts.

10. The display device in accordance with claim 9, wherein a first partition is displayed in one frame in a time order different than displayed in a next frame but wherein the timing between display of the first partition in each frame does not deviate substantially from the frame period.

11. A television receiver comprising a display device as claimed in any of the claims 1-6.

12. A method for decrypting and displaying encrypted video pixel data, comprising the steps of:

receiving encrypted video pixel data including digital code for each pixel to be displayed decrypted on an array of p columns by l rows of pixel cells as a frame;

storing at least a portion of a frame of the digital code of the encrypted video pixel data in a register, such that the encrypted video data is stored in the register in an encrypted order rather than in a column or row sequential order;

decrypting the encrypted video pixel data in accordance with a decryption key and supplying the decrypted video data to a driver circuit;

providing the decrypted video pixel data from the driver circuit to an array of memory elements having p columns and l rows of memory elements each memory element being associated with a particular pixel cell to store the digital code of the decrypted video pixel data which represents the luminance of the particular pixel cell during a frame period; and

wherein the step of providing requires activating the columns of the array of memory elements for loading the memory elements with the sorted digital code from the driver circuit, and activating the rows of the array of memory elements, one row at a time, non-sequentially in accordance with the decryption key.

13. A method for decrypting and displaying encrypted digital video pixel data, comprising the steps of:

receiving encrypted video data to be displayed decrypted on an array of p columns by l rows of pixel cells;

storing in a register a line of a frame of digital video pixel data in a n encrypted order rather than in a column sequential order;

decrypting the encrypted video pixel date in accordance with a decryption key and supplying the decrypted video data to a driver circuit;

providing the decrypted video pixel data from the driver circuit to an array of memory elements having p columns and l rows of memory elements each memory element being associated with a particular pixel cell to store the digital code of the decrypted digital video pixel data which represents the luminance of the particular pixel cell during a frame period; and

wherein the step of providing requires activating the columns of the array of memory elements with the stored digital code from the driver circuit; and activating sequentially one row at a time for each line of digital code.

14. A method of encrypting video pixel data for display on an LCD, comprising the steps of:

partitioning each frame of video pixel data into a plurality of predetermined partitions, each partition having a plurality of rows of pixel data;

encrypting the rows by altering the time sequence of display of the rows within a partition but not the time sequence of the partitions; and

providing the encrypted video pixel data to an LCD.

15. The method as claimed in claim 16, wherein the time sequence of the partitions are also altered such that the partitions are displayed by the LCD non-sequentially in accordance with a time-sequence that minimizes temporal artifacts.

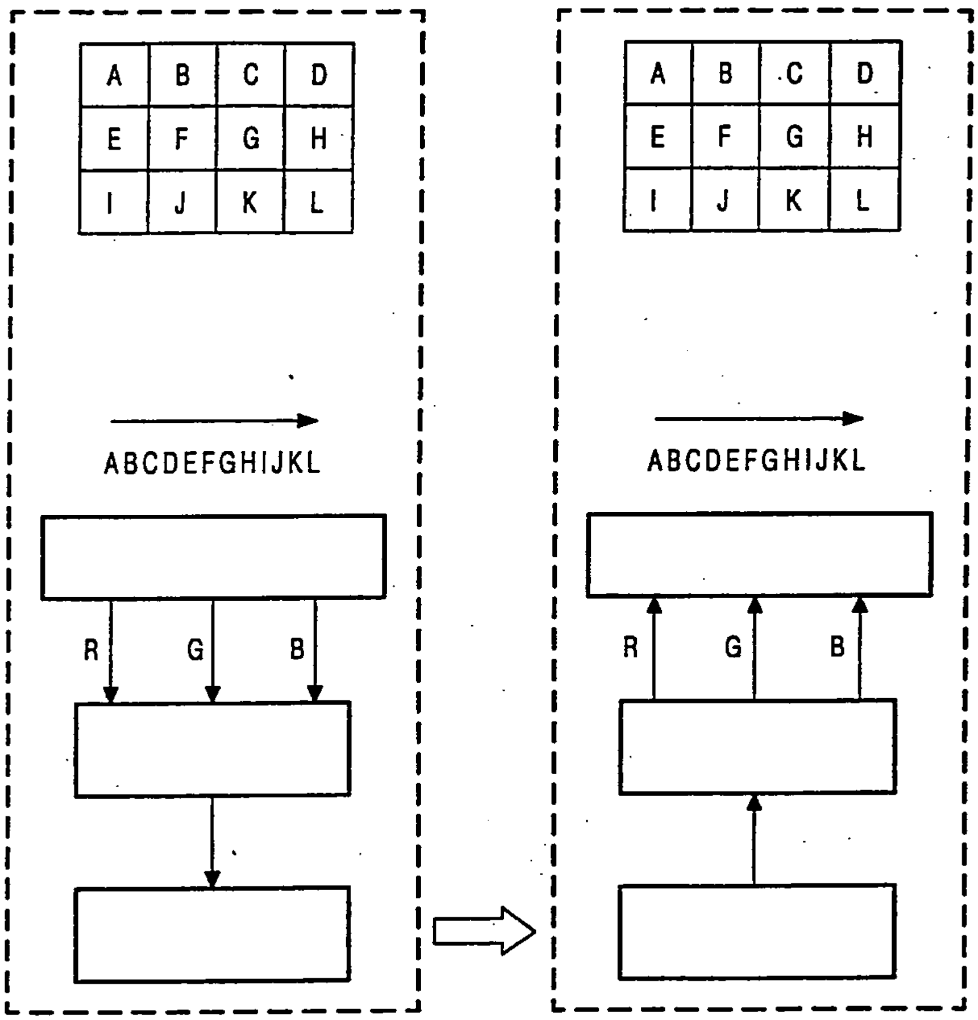
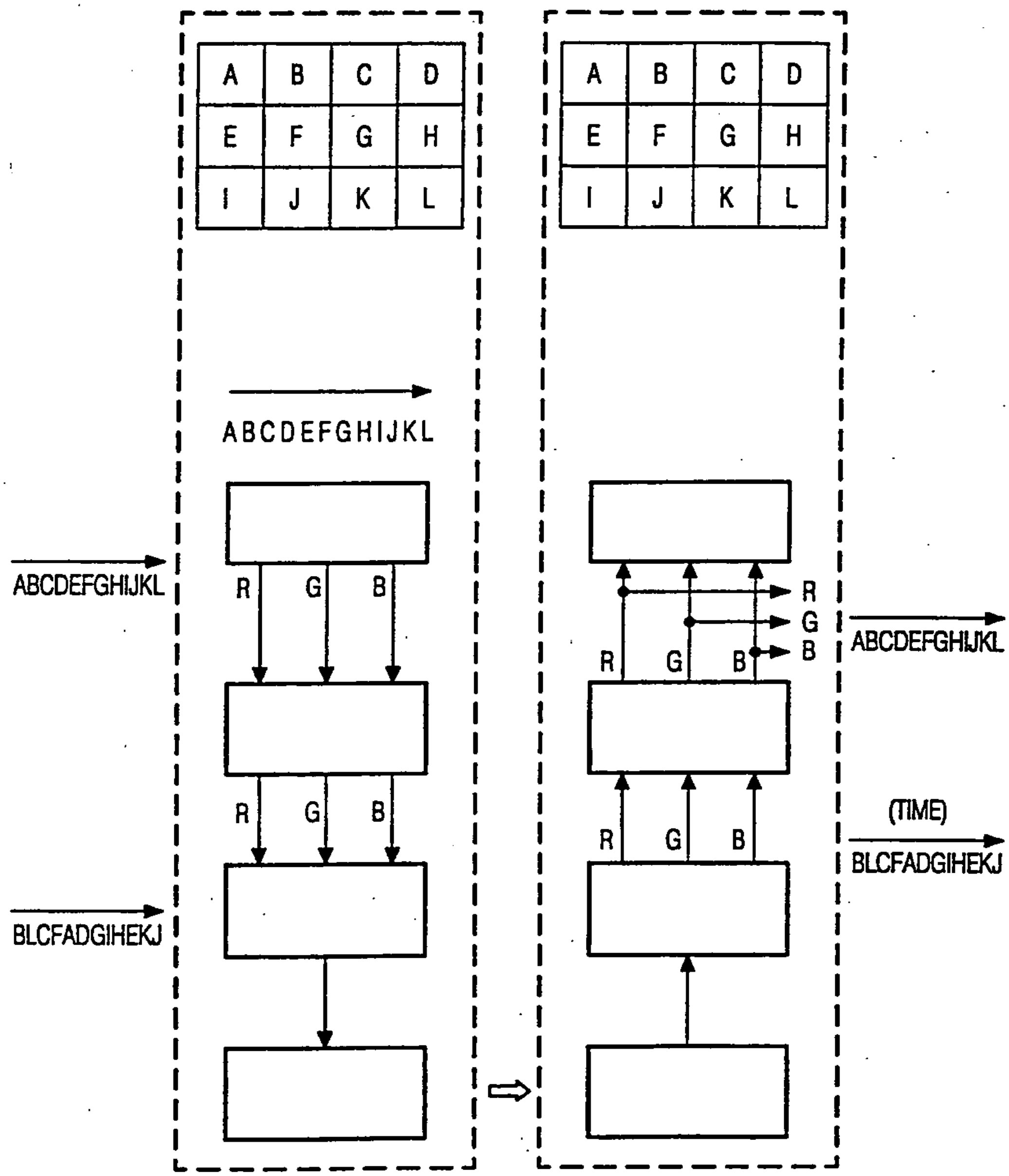

A B C D
E F G H
I J K L
ABCDEFGHIJKL
R
G
B
A B C D
E F G H
I J K L
ABCDEFGHIJKL
R
G
B

FIG. 1



A B C D
E F G H
I J K L
ABCDEFGHIJKL
ABCDEFGHIJKL
R G B
R G B
BLCFADGIHEKJ
A B C D
E F G H
I J K L
R
G
B
R G B
ABCDEFGHIJKL
R G B
(TIME)
BLCFADGIHEKJ

FIG. 2

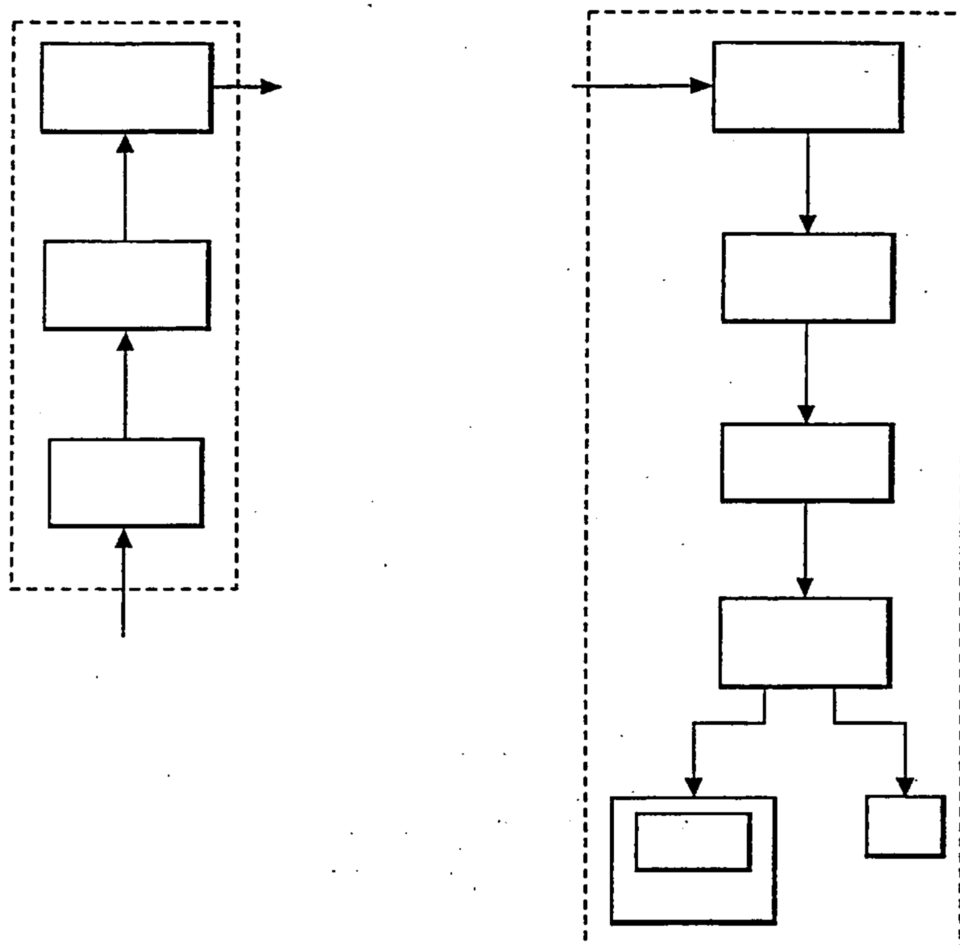


FIG. 3

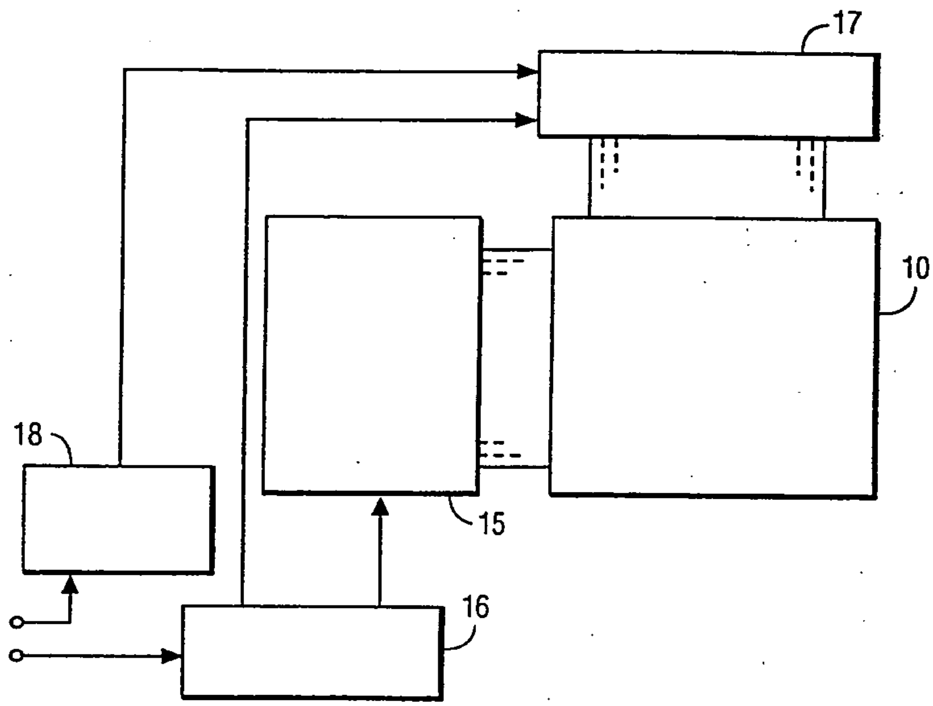


FIG. 4

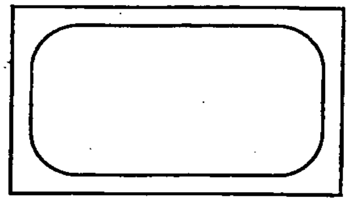


FIG. 5A

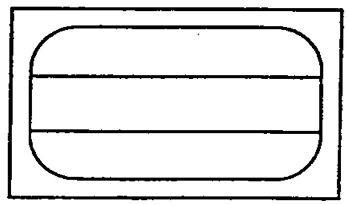


FIG. 5B

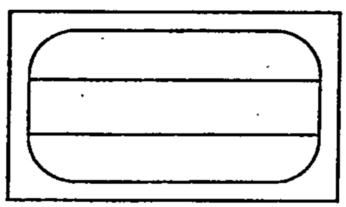


FIG. 5C

A	1	1	1	1	1	1	1	1	
B	2	2	2	2	2	2	2	2	• • •
C	3	3	3	3	3	3	3	3	

FIG. 5D

A	1	1	1	1	1	1	1	1
B	2	2	2	2	2	2	2	2
C	3	3	3	3	3	3	3	3

FIG. 6A

A	1	1	2	2	3	3	1	3
B	2	3	1	3	1	2	2	2
C	3	2	3	1	2	1	3	1

FIG. 6B

A	1	1	2	3	3	2	1	2
B	2	3	3	2	1	1	2	1
C	3	2	1	1	2	3	3	3

FIG. 6C

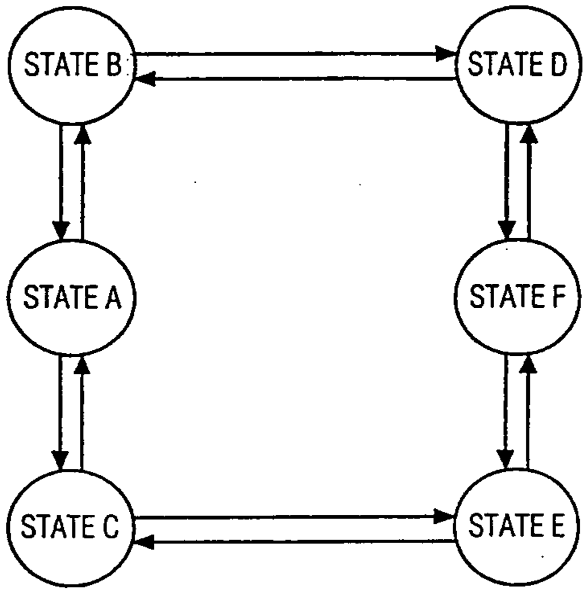


FIG. 7A

SECTION	STATE A	STATE B	STATE D	STATE F	STATE E	STATE C	STATE A	STATE C
A	1	1	2	3	3	2	1	2
B	2	3	3	2	1	1	2	1
C	3	2	1	1	2	3	3	3
	FRAME 1	FRAME 2	FRAME 3	FRAME 4	FRAME 5	FRAME 6	FRAME 7	FRAME 8

FRAME TIME

FIG. 7B

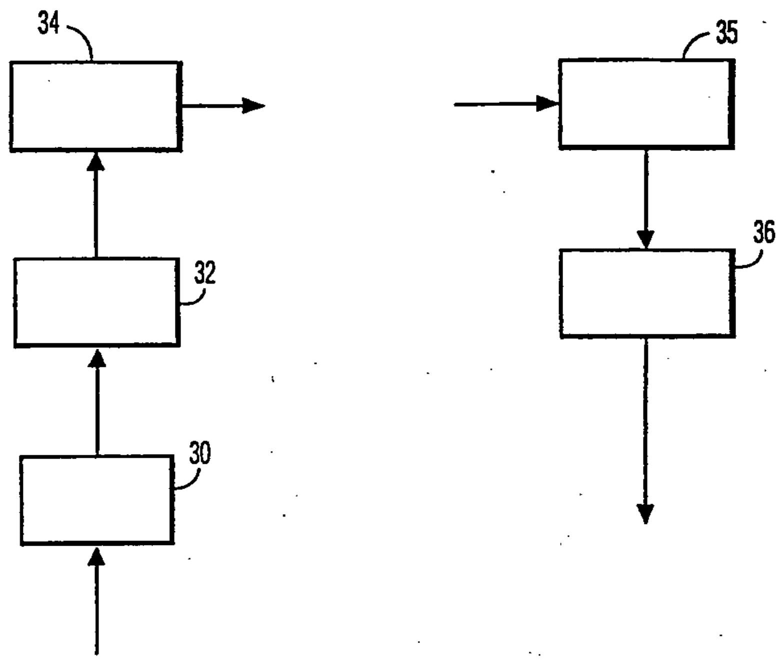


FIG. 8